Bundesministerium
des Innern

Freiheit
Einheit
Demokratie

Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)

Nationale Strategie zum Schutz Kritischer Infrastrukturen

1. Leitbild

Infrastrukturen im Allgemeinen und Kritische Infrastrukturen im Besonderen sind die unverzichtbaren Lebensadern moderner, leistungsfähiger Gesellschaften. Deutschland gehört zu den führenden industriell und technologisch geprägten Nationen. Die Bedeutung des Wirtschaftsstandortes Deutschland und die Sicherstellung der Wettbewerbsfähigkeit in einer globalisierten Welt als Voraussetzungen für Wohlstand und Fortschritt sind maßgeblich vom Vorhandensein hochleistungsfähiger und funktionstüchtiger Infrastrukturen abhängig.

Die Gewährleistung des Schutzes dieser Infrastrukturen ist daher eine Kernaufgabe staatlicher und unternehmerischer Sicherheitsvorsorge und zentrales Thema der Sicherheitspolitik unseres Landes. Deutschland hat sich sowohl national als auch international des Schutzes Kritischer Infrastrukturen aktiv angenommen und wird vom Grundsatz gemeinschaftlichen Handelns von Staat, Gesellschaft und Wirtschaft geleitet. Der Staat kooperiert partnerschaftlich mit anderen öffentlichen und privaten Akteuren bei der Erarbeitung von Analysen und Schutzkonzeptionen. Er steuert primär moderierend, nötigenfalls normierend, die Maßnahmen zur Sicherung und zur Sicherstellung des Gesamtsystems sowie der Systemabläufe.

Die Umsetzung von Maßnahmen zum Infrastrukturschutz auf der Grundlage freiwilliger Vereinbarungen sowie als Gegenstand der Gesetzgebung hat dazu beigetragen, dass sich der Sicherheitsstandard und die Ausfallsicherheit Kritischer Infrastrukturen in Deutschland auf einem hohen Niveau bewegen. Um diesem Niveau angesichts veränderter Rahmenbedingungen auch künftig entsprechen zu können, ist der bisher beschrittene Weg einer vertrauensvollen und konstruktiven Kooperation zum umfassenden Schutz Kritischer Infrastrukturen fortzusetzen und die Zusammenarbeit der relevanten Akteure aus Staat und Wirtschaft zu vertiefen und auszubauen.

Die „Nationale Strategie zum Schutz Kritischer Infrastrukturen“ fasst die Zielvorstellungen und den politisch-strategischen Ansatz des Bundes, wie er bereits praktiziert wird und sich beispielsweise auch im „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ (NPSI) für den Bereich der Informationstechnik wieder findet, zusammen und ist Ausgangspunkt, das bislang Erreichte auf konsolidierter Grundlage fortzusetzen und mit Blick auf neue Herausforderungen weiterzuentwickeln.

●●●

2. Bisherige Bilanz

Der Schutz Kritischer Infrastrukturen ist eine gesamtgesellschaftliche Aufgabe, die ein abgestimmtes und von allen Verantwortlichen – Staat, Wirtschaft und Öffentlichkeit – unterstütztes Vorgehen erfordert. Die Bedeutung dieser Aufgabe leitet sich unmittelbar aus der im Bund verwendeten Definition für den Begriff „Kritische Infrastrukturen“ ab:

Definition

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Deutschland ist von einem engmaschigen Netz gesellschaftswichtiger Infrastrukturen durchzogen. Die Versorgung der Bevölkerung und der Unternehmen mit Energie-, IT- und Transportdienstleistungen, mit Einrichtungen des Gesundheits- und des Finanzwesens sowie im Bereich des Trinkwassers und der Ernährung ist sehr gut. Ein stabiles Verfassungs- und Rechtssystem gewährleistet die Rahmenbedingungen für ein friedliches Zusammenleben in Sicherheit und Wohlstand auch in Krisenfällen.

Neben quantitativen Aspekten ist Deutschland auch in qualitativer Hinsicht gut aufgestellt. Die Versorgungssicherheit im Sinne einer Ausfallsicherheit etwa im Bereich der Stromversorgung nimmt im Vergleich zu anderen Staaten einen der oberen Plätze ein. Denn die privatwirtschaftlich organisierten Energieversorgungsunternehmen sind gesetzlich verpflichtet, ein sicheres, zuverlässiges und leistungsfähiges Versorgungsnetz zu betreiben. Die Einhaltung der Anforderungen wird von den Verbänden auf Basis des Energiewirtschaftsgesetzes und von staatlicher Seite durch die Bundesnetzagentur insbesondere mittels technischer Überprüfungen und Monitoringberichten überwacht. In vergleichbarer Weise unterliegen auch Telekommunikations(TK)–Diensteanbieter gesetzlichen Regelungen und müssen durch technische Vorkehrungen und sonstige Maßnahmen die TK- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe schützen. Weiterhin müssen die Betreiber von TK-Anlagen einen Sicherheitsbeauftragten benennen und der Bundesnetzagentur ein Sicherheitskonzept vorlegen, aus dem hervorgehen muss, von welchen Gefährdungen auszugehen ist und welche technische Vorkehrungen oder sonstige Schutzmaßnahmen getroffen oder geplant sind.

Doch ist die gesellschaftliche Verletzlichkeit aufgrund des zunehmenden Durchdringungs- und Abhängigkeitsgrades nahezu sämtlicher Lebensbereiche mit und von Kritischen Infrastrukturen in den vergangenen Jahren rapide angestiegen. Damit nehmen Aspekte der Inneren Sicherheit in diesem Themenfeld einen sehr hohen und auch weiter wachsenden Stellenwert ein.

Die Bundesregierung stellt sich bereits seit Ende der 90er Jahre der Gewährleistung des Schutzes Kritischer Infrastrukturen als Kernaufgabe staatlicher Sicherheitsvorsorge. Dabei spielen neben von den Fachressorts wahrgenommenen sektoralen Aspekten auch und insbesondere sektorübergreifende Fragen eine gewichtige Rolle.

Die zentralen bundesstaatlichen Maßnahmen zum Schutz Kritischer Infrastrukturen werden im Bundesministerium des Innern (BMI) ressortübergreifend koordiniert. Die Geschäftsbereichsbehörden des BMI, wie das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundeskriminalamt (BKA) und die Bundesanstalt Technisches Hilfswerk (THW) erarbeiten im ministeriellen Auftrag Gefährdungsbewertungen, Analysen und Schutzkonzepte.

Ergebnisse

Insgesamt wurden zahlreiche Initiativen ergriffen und Maßnahmenpakete umgesetzt. Beispiele hierfür sind:

- Umfassende Vorsorgemaßnahmen von Staat und Wirtschaft wurden zur Bewältigung des so genannten „Jahr 2000-Problems“ getroffen, um die Funktionsfähigkeit der Informationstechnik und aller computergestützten Infrastrukturen auch nach dem Jahrtausendwechsel zu gewährleisten. Mit dem IT-Grundschutz für die Informationsinfrastrukturen, mit dem Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI) sowie dem darauf aufbauenden Umsetzungsplan KRITIS (UP KRITIS) sind wichtige Konzepte und konkrete Maßnahmen erarbeitet worden. Die Umsetzung erfolgt gemeinschaftlich mit der Wirtschaft.

- Mit den Terroranschlägen vom 11. September 2001 sowie dem Sommerhochwasser von 2002 sind neben der Informationstechnik auch alle anderen Kritischen Infrastrukturen in den Fokus strukturierter staatlicher Sicherheitsvorsorge gerückt. Bei der Betrachtung möglicher Gefährdungen wurden neue Schwerpunkte gesetzt. Wichtige Änderungen in Folge des 11. September 2001 waren beispielsweise die Einführung des vorbeugenden per-

sonellen Sabotageschutzes, zu dem bestimmte öffentliche und nicht-öffentliche Einrichtungen verpflichtet sind, oder die internationalen Übereinkommen zu erhöhten Schutzmaßnahmen im Verkehrssektor, z. B. bei Flughäfen oder Hafeninfrastrukturen, die in Deutschland umgesetzt wurden.

- Ergebnisse des Zusammenwirkens von öffentlichem und privatem Sektor sind neben den IT-Sicherheitskonzepten eine Reihe weiterer Empfehlungen, Leitfäden und Handreichungen, die in enger Kooperation mit Behörden, Infrastrukturunternehmen sowie mit Verbänden, mit der Industrie und der Wissenschaft erarbeitet wurden. Hierzu zählen beispielsweise die Leitfäden „Schutz Kritischer Infrastrukturen – Basisschutzkonzept“ und „Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement“, Schutzkonzepte für Hilfsorganisationen, Wohlfahrtsverbände und Krankenhäuser, oder das „Handbuch betriebliche Pandemieplanung“.

- Darüber hinaus werden Infrastrukturunternehmen regelmäßig eingeladen, an der seit 2004 stattfindenden Bund-Länder-Krisenmanagementübung „LÜKEX“ teilzunehmen mit dem Ziel, die zur Krisenbewältigung aufgebauten Strukturen und Maßnahmen staatlicher *und* privater Partner als Baustein der gesamtstaatlichen Sicherheitsvorsorge kennen zu lernen, zu beüben und weiterzuentwickeln. Diese gemeinsamen Übungen haben die vertrauensvolle Zusammenarbeit von Staat und Wirtschaft vertieft in der Überzeugung, dass Krisenfälle nur gemeinsam zu bewältigen sind.

- Um den veränderten Risiken und wachsenden Verletzlichkeiten künftig noch stärker als bisher vorbeugend zu begegnen sowie das Potential neuer Technologien und Verfahren für den Schutz Kritischer Infrastrukturen optimal zu erschließen, beteiligen sich die Behörden des Bundes umfangreich an dem Programm „Forschung für die zivile Sicherheit“, welches die Bundesregierung in 2007 als Teil der Hightech-Strategie für Deutschland gestartet hat. Im Verbund mit Wissenschaft, Industrie und Infrastrukturbetreibern werden innovative Lösungen für die zivile Sicherheit erforscht und entwickelt.

Dieses mittlerweile engmaschige Netzwerk für Informations- und Kommunikationsflüsse zwischen Staat und Unternehmen und für gemeinsame Projekte und Maßnahmen gilt es, wo nötig, weiter auszubauen und zu vertiefen.

●●●

3. Kritikalität von Infrastrukturen und Verantwortungsbereiche

Infrastrukturen gelten dann als „kritisch“, wenn sie für die Funktionsfähigkeit moderner Gesellschaften von wichtiger Bedeutung sind und ihr Ausfall oder ihre Beeinträchtigung nachhaltige Störungen im Gesamtsystem zur Folge hat. Ein wichtiges Kriterium dafür ist die Kritikalität als

Definition Kritikalität

> *relatives Maß für die Bedeutsamkeit einer Infrastruktur in Bezug auf die Konsequenzen, die eine Störung oder ein Funktionsausfall für die Versorgungssicherheit der Gesellschaft mit wichtigen Gütern und Dienstleistungen hat.*

Diese Kritikalität kann systemischen oder symbolischen Charakter haben oder auch beide Charakteristika aufweisen. Eine Infrastruktur besitzt vor allem dann eine *systemische Kritikalität*, wenn sie aufgrund ihrer strukturellen, funktionellen und technischen Positionierung im Gesamtsystem der Infrastrukturbereiche von besonders hoher interdependenter Relevanz ist. Beispiele dafür sind die *Elektrizitäts-* sowie *Informations- und Telekommunikationsinfrastrukturen*, die aufgrund ihrer Vernetzungsgröße und Vernetzungsstärke besonders relevant sind und bei großflächigem und lange anhaltendem Ausfall zu gravierenden Störungen der gesellschaftlichen Abläufe sowie der öffentlichen Sicherheit führen können. Eine *symbolische Kritikalität* kann eine Infrastruktur dann besitzen, wenn aufgrund ihrer kulturellen oder identitätsstiftenden Bedeutung ihre Zerstörung eine Gesellschaft emotional erschüttern und psychologisch nachhaltig aus dem Gleichgewicht bringen kann.

Kritische Infrastrukturen können aufgrund ihrer technischen, strukturellen und funktionellen Spezifika in unverzichtbare technische Basisinfrastrukturen und unverzichtbare sozioökonomische Dienstleistungsinfrastrukturen unterschieden werden. Zu diesen gehören in Deutschland:

Technische Basisinfrastrukturen	Sozioökonomische Dienstleistungsinfrastrukturen
Energieversorgung	Gesundheitswesen, Ernährung
Informations- und Kommunikations-technologie	Notfall- und Rettungswesen, Katastrophenschutz
Transport und Verkehr	Parlament, Regierung, öffentliche Verwaltung, Justizeinrichtungen
(Trink-) Wasserversorgung und Abwasserentsorgung	Finanz- und Versicherungswesen
	Medien und Kulturgüter

Zwischen beiden Infrastrukturbereichen bestehen grundsätzlich erhebliche Abhängigkeiten, da nahezu alle sozioökonomischen Dienstleistungsinfrastrukturen der weitgehend uneingeschränkten Verfügbarkeit der technischen Basisinfrastrukturen bedürfen. Aber auch umgekehrt sind technische Basisinfrastrukturen auf sozioökonomische Dienstleistungsinfrastrukturen wie etwa ein stabiles Rechtssystem oder ein funktionsfähiges Notfall- und Rettungswesen im Krisenfall angewiesen.

Betrachtet man die einzelnen Infrastrukturen unter Aspekten der Eigentumsverhältnisse, wird deutlich, dass es sich in der Regel nicht um staatliche Einrichtungen handelt, sondern die Mehrheit dieser Infrastrukturen von privaten - zum Teil erst kürzlich privatisierten - Unternehmen betrieben und gesteuert wird.

Gleiches gilt in wachsendem Maße auch für die zahlreichen öffentlichen Infrastrukturdienstleistungen der kommunalen Ebene, die mehr und mehr in privatrechtlich organisierten Unternehmensformen erbracht werden.

Verantwortung für KRITIS

Mit diesem Trend geht auch die Verantwortung für die Sicherheit, Zuverlässigkeit und Verfügbarkeit dieser Infrastrukturen zunehmend in private, zumindest aber geteilte Verantwortung über. Staatliche Aufgaben bzw. Aufgaben der öffentlichen Hand bewegen sich damit vorrangig im Rahmen einer Gewährleistung, allenfalls der Sicherstellung der Versorgung in Krisenzeiten, wenn übliche Marktmechanismen nicht mehr funktionieren. Zur Vorsorge vor und zur Überbrückung von bedenklichen Störungen und gravierenden Schadensereignissen bedarf es daher einer institutionalisierten, organisierten Zusammenarbeit von Staat und Wirtschaft in etablierten Sicherheitspartnerschaften.

●●●

4. Gefährdungen, Risiken, Verletzlichkeiten, Risiken und Risikokultur

Kritische Infrastrukturen können durch verschiedene Gefahren bedroht sein, die bei Risiko- und Gefährdungsanalysen sowie der Auswahl von Handlungsoptionen gleichermaßen zu berücksichtigen sind (All-Gefahren-Ansatz). Das Gesamtspektrum der Gefahren lässt sich wie folgt abbilden:

Naturereignisse	**Technisches / menschliches Versagen**	**Terrorismus, Kriminalität, Krieg**
Extremwetterereignisse u.a. Stürme, Starkniederschläge, Temperaturstürze, Hochwasser, Hitzewellen, Dürren	Systemversagen u.a. Unter- und Überkomplexität in der Planung, Hardware-, Softwarefehler	Terrorismus
Wald- und Heidebrände	Fahrlässigkeit	Sabotage
Seismische Ereignisse	Unfälle und Havarien	sonstige Kriminalität
Epidemien und Pandemien bei Mensch, Tier und Pflanzen	Organisatorisches Versagen u.a. Defizite im Risiko- und Krisenmanagement, unzureichende Koordination und Kooperation	Bürgerkriege und Kriege
Kosmische Ereignisse u. a. kosmische Energiestürme, Meteoriten und Kometen		

Diese Ereignisse mit sehr unterschiedlichen Ursachen können die für die Gesellschaft und den einzelnen Bürger lebenswichtigen Infrastruktureinrichtungen beeinträchtigen, massiv schädigen oder zerstören. Durch die große Abhängigkeit von infrastrukturellen Dienstleistungen ist die Gesellschaft sehr verletzlich geworden, wobei diese Verletzlichkeit nicht nur durch Gefahren und Risiken von Außen, sondern auch aufgrund der hohen Interdependenzen zwischen den einzelnen Infrastruktursystemen im Innern stark angewachsen ist. Die Folge von Störungen oder Ausfällen können so genannte Domino- und Kaskadeneffekte sein, die das Potential besitzen, gesellschaftliche Teilbereiche zum Erliegen zu bringen, und die neben dem unmittelbaren Schaden für betroffene Menschen enorme volkswirtschaftliche Schäden sowie Vertrauensverluste in die politische Führung einer Gesellschaft bewirken können.

Seit dem 11. September 2001 ist vor allem die Bedrohung durch den internationalen Terrorismus die Haupttriebfeder staatlicher Schutz- und Sicherheitsanstrengungen. Diese Bedrohung hat in den letzten Jahren weiter an Bedeutung

gewonnen. Die zunehmende Nutzung moderner Techniken durch (potentielle) terroristische Gewalttäter in Verbindung mit gesellschaftlichen Abhängigkeiten von zuverlässigen Infrastrukturen macht kontinuierliche Maßnahmen zum Schutz Kritischer Infrastrukturen vor terroristischen Anschlägen notwendig.

Neben den aus vorsätzlichen, insbesondere terroristischen Handlungen resultierenden Risiken sind aber auch mögliche, teils immense Schäden an Infrastrukturen durch natürliche Extremereignisse zu beachten. In Deutschland sind es vor allem Wetterextreme, wie schwere Stürme oder Starkniederschläge, die die Infrastruktureinrichtungen und damit die Versorgungsleistungen schwer schädigen können. Der wissenschaftlich untermauerte und in seinen Auswirkungen immer stärker zu spürende Klimawandel wird die Weltgemeinschaft zukünftig langfristig und intensiv beschäftigen. Auch wenn die Folgen insgesamt noch nicht vollständig absehbar sind, werden die klimatischen Veränderungen weitere, teils extreme Belastungen für die Kritischen Infrastrukturen auch in den bisher gemäßigten Breitengraden Mitteleuropas mit sich bringen.

Die staatliche und gesellschaftliche Aufmerksamkeit muss deshalb vor allem zwei Gefährdungsursachen gelten: einmal der terroristischen Bedrohung und darüber hinaus den in ihrer Bedeutung für die Infrastrukturen wachsenden Naturgefahren.

Gleichermaßen bedeutsam sind die Risiken und Gefährdungen für Informationsinfrastrukturen. Kriminelle Handlungen, technisches bzw. menschliches Versagen oder organisatorische Mängel gefährden die Funktionsfähigkeit dieser für moderne Gesellschaften und ihre Betriebsabläufe unverzichtbaren Infrastruktur, deren Störung oder Ausfall aufgrund der Interdependenzen weit reichende Folgen nach sich ziehen kann.

Unabhängig von Art und Ursachen der einzelnen Gefährdungen sind besonders hoch industrialisierte, sehr komplexe Technologien nutzende und auf arbeitsteiligen, ausdifferenzierten Organisationsstrukturen aufbauende Gesellschaften auch aufgrund dieses Umstandes besonders verletzlich. Gesellschaften reagieren im Laufe ihrer technologischen Entwicklung auf Störungen vor allem der auf hoch entwickelten Technologien basierenden Infrastrukturen deutlich sensibler, da sie sehr hohe Sicherheitsstandards und eine hohe Versorgungssicherheit gewohnt sind. Dieser Umstand, dass sich mit zunehmender Robustheit und geringerer Störanfälligkeit ein durchaus trügerisches Gefühl von Sicherheit entwickelt und die Auswirkungen eines „Dennoch-Störfalls“ überproportional hoch sind, wird als Verletzlichkeitsparadoxon bezeichnet:

Verletzlichkeits-paradoxon

In dem Maße, in dem ein Land in seinen Versorgungsleistungen weniger störanfällig ist, wirkt sich jede Störung umso stärker aus.

Dieses Paradoxon wird kontinuierlich verstärkt, in dem in nahezu allen gesellschaftlichen Bereichen elektrische bzw. elektronische Geräte, Mess- und Regelungstechnik, Informations- und Kommunikationstechnologien weiter zunehmen und die Abhängigkeit z.B. von der Verfügbarkeit elektrischen Stroms oder aber von Informations- und Kommunikationstechniken weiter wächst. Technikfolgen-Abschätzungen sollten daher auch unter dem Aspekt sicherheitspolitischer Überlegungen zum Schutz Kritischer Infrastrukturen weiter an Bedeutung gewinnen.

Eine Schlussfolgerung aus den erkannten neuen Gefährdungen, Risiken und hohen Verletzlichkeiten und der damit verbundenen Komplexität bei Prävention und Schutzvorkehr ist allerdings auch hinsichtlich der bisher üblichen Sicherheitsphilosophie zu ziehen:

Risikokultur

Ein 100%-iger Schutz der Infrastrukturen und ihrer Leistungsfähigkeit ist weder von Seiten des Staates, noch von Seiten der Betreiber zu gewährleisten. Das bisherige Sicherheitsdenken muss sich hin zu einer neuen „Risikokultur“ transformieren. Diese neue Risikokultur basiert unter anderem auf

- einer offenen Risikokommunikation zwischen Staat, Unternehmen, Bürgern und Öffentlichkeit unter Berücksichtigung der Sensibilität bestimmter Informationen,
- der Zusammenarbeit aller relevanten Akteure bei der Prävention und Bewältigung von Ereignissen,
- der verstärkten Selbstverpflichtung der Betreiber zur Prävention und zur Bewältigung von Ereignissen,
- einer verstärkten und selbstbewussten Selbstschutz- und Selbsthilfefähigkeit der von Störungen oder dem Ausfall Kritischer Infrastrukturleistungen betroffenen Menschen und Einrichtungen.

Eine solche neue Risikokultur ist geeignet, die Gesellschaft im Umgang mit wachsenden Verletzlichkeiten robuster und widerstandsfähiger zu gestalten.

●●●

5. Strategische Ziele

Der Schutz Kritischer Infrastrukturen in Deutschland ist eine Aufgabe, die Staat, Unternehmen bzw. Betreiber und auch die Öffentlichkeit gemeinsam zu bewältigen haben. Leitprinzipien beim Schutz Kritischer Infrastrukturen sind insbesondere

- eine vertrauensvolle Kooperation zwischen Staat und Wirtschaft auf allen Ebenen und
- die Erforderlichkeit, Geeignetheit und Verhältnismäßigkeit der Maßnahmen und des Mitteleinsatzes zur Erhöhung des Schutzniveaus.

Um das gemeinsame Handeln zum Erfolg zu führen, sind strategische Zielvorstellungen notwendig, die das grundsätzliche Denken, Handeln und Verhalten in allen wesentlichen sicherheitspolitischen Fragestellungen zum Schutz Kritischer Infrastrukturen gegenüber allen relevanten Risiken beschreiben. Daraus lassen sich Teilziele entwickeln, die wiederum in Programmen, Plänen oder Konzepten umgesetzt werden. Im Bereich IT existiert mit dem NPSI bereits ein solcher Plan.

Die staatlichen Anstrengungen zum Schutz Kritischer Infrastrukturen müssen darauf gerichtet sein, das Schutzniveau in Deutschland durch geeignete und mit den anderen Akteuren abgestimmte Maßnahmen so zu sichern und zu erhöhen, dass

- alle vorhandenen und zu erwartenden Risiken im Vorfeld erkannt sowie kritische Elemente und Prozesse identifiziert werden, gravierende Störungen und Ausfälle von wichtigen Infrastrukturleistungen durch eine umfassende Schutzvorkehr möglichst vermieden und durch ein vorhandenes effizientes Risiko- und Krisenmanagement sowie adäquate Handlungsoptionen auf ein Mindestmaß beschränkt werden; die getroffenen Maßnahmen sollten, soweit möglich, regelmäßig Bestandteil von Übungen sein,

Prävention

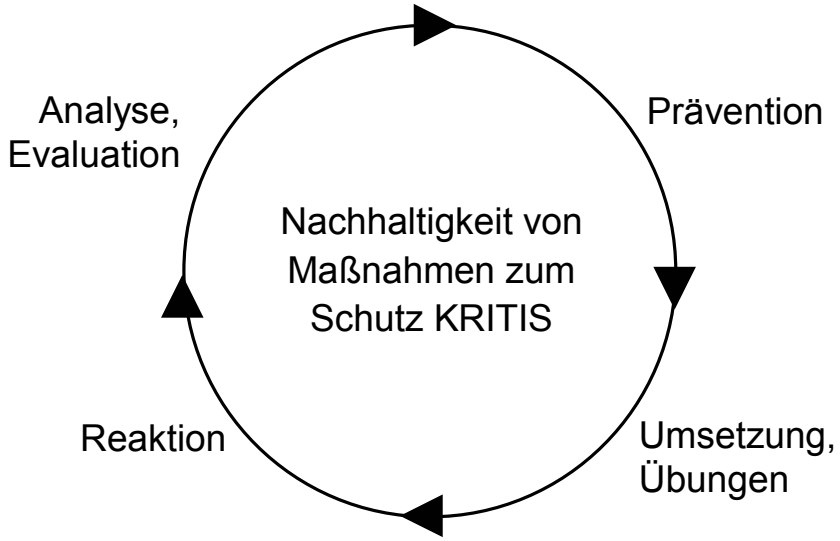
- Folgen von gravierenden Störungen und Ausfällen durch ein effektives Notfall- und Krisenmanagement und effiziente Redundanzen sowie eine wirkungsvolle Selbsthilfekapazität der unmittelbar Betroffenen so gering wie möglich gehalten werden; alle Aktivitäten im Stör- oder Schadensfall müssen darauf ausgerichtet sein, über ein Höchstmaß an Wirkung zu verfügen, damit der Regelbetrieb möglichst umgehend wieder aufgenommen werden kann.

Reaktion

Nachhaltigkeit

- Darüber hinaus müssen aus laufend fortgeschriebenen Gefährdungsanalysen sowie den Analysen von Störfällen und anderen Ereignissen im In- und Ausland Erfahrungen für den verbesserten Schutz Kritischer Infrastrukturen gewonnen und in gemeinsam mit den Betreibern zu entwickelnden sowie im internationalen Kontext abgestimmten Schutzstandards umgesetzt werden.

Die konsequente Umsetzung dieser Ziele in Form eines Risikomanagement-Kreislaufes für Kritische Infrastrukturen bietet die notwendige Gewähr für ein in sich geschlossenes nachhaltig wirkendes Schutzsystem, durch das die deutschen Sicherheitskompetenzen gestärkt werden und in den internationalen Erfahrungsaustausch einfließen.



●●●

6. Zusammenarbeit, Selbstverpflichtung und Rechtsetzung

Für den Erfolg bei der Umsetzung der strategischen Ziele sind funktionierende Kooperationen und Partnerschaften sowohl mit und zwischen Behörden unterschiedlicher Ressort- und Ebenenzugehörigkeit als auch mit und zwischen den überwiegend privatrechtlich organisierten und privatwirtschaftlich arbeitenden Infrastrukturbetreibern sowie den Verbänden als Multiplikatoren eine grundlegende Voraussetzung. Nicht zuletzt im Zusammenhang mit dem von der Bundesregierung initiierten und vom Bundesministerium für Bildung und Forschung betreuten nationalen Programm „Forschung für die zivile Sicherheit“ sowie mit der europäischen Sicherheitsforschung sind auch andere gesellschaftliche Akteure von Bedeutung wie z.B. die Wissenschaft und die Industrie.

Zur Stärkung des Schutzes Kritischer Infrastrukturen bedarf es daher einer intensiven Zusammenarbeit, Abstimmung und Information zwischen und unter den Partnern und Akteuren, zu denen vor allem

- der Bund mit seinen Behörden,
- die Länder mit ihren Behörden,
- die Landkreise und Kommunen mit ihren Ämtern,
- die Betreiber der Infrastrukturen,
- die Hilfeleistungsorganisationen,
- die Wirtschafts- und Fachverbände,
- die Wissenschaft und Forschung,
- die (Sicherheits-) Industrie,
- die Öffentlichkeit (Bevölkerung, Medien),
- internationale und supranationale Einrichtungen

und bei Bedarf weitere Institutionen gehören.

Kooperativer Ansatz

Der Schutz Kritischer Infrastrukturen erfordert das Zusammenwirken der einzelnen Ressorts auf Bundesebene innerhalb ihrer Zuständigkeiten und der staatlichen Ebenen im Rahmen der Kompetenzverteilung. Dazu gehören der allseitige Informationsaustausch und die Entwicklung von abgestimmten Handlungskonzepten mit den Infrastrukturunternehmen. Der Bund bekennt sich zu einem kooperativen Ansatz und erwartet, dass wichtige gemeinsam erarbeitete analytische Erkenntnisse, Rahmenempfehlungen und Schutzkonzepte durch die Infra-

strukturunternehmen und Betreiber sowie durch andere wichtige Akteure, wie beispielsweise Verbände oder Normungsausschüsse, entsprechend den Sicherheitserfordernissen umgesetzt werden.

Staatlicher Vorbehalt

Sofern erhebliche festgestellte Sicherheitsmängel in Kritischen Infrastrukturbereichen durch die freiwillige Selbstverpflichtung der Unternehmen nicht beseitigt werden oder bestehende gesetzliche Regelungen im Umfeld der Anlagen-, Netz-, Betreiber- oder Nutzersicherheit aufgrund neuer Gefahren und Risiken nicht ausreichenden Schutz bieten oder Anwendung finden, behält es sich der Bund für seinen Zuständigkeitsbereich vor, durch geänderte oder neue Rechtsetzung den Schutz der betreffenden Infrastrukturen zu optimieren.

●●●

7. Umsetzungsverfahren

Bund, Länder und Kommunen sind *gemeinsam* gefordert, den Schutz Kritischer Infrastrukturen zu fördern und in ihren Zuständigkeitsbereichen umzusetzen. Dafür ist ein strukturiertes Umsetzungsverfahren auf den drei Verwaltungsebenen geeignet, das unter Bezugnahme auf den vom Bund gewählten kooperativen Ansatz unter Beteiligung der anderen maßgeblichen Akteure – Betreiber, Verbände – aus folgenden, teilweise parallel laufenden Arbeitspaketen besteht:

Arbeitspakete

1. Festlegung allgemeiner Schutzziele.
2. Analyse von Gefährdungen, Verwundbarkeiten und Bewältigungskapazitäten.
3. Bewertung der Gefährdungen.
4. Konkretisierung der Schutzziele unter Einbeziehung vorhandener Schutzmaßnahmen; Analyse vorhandener Regelungen und ggf. Ableitung weiterer Maßnahmen zur Zielerreichung; ggf. Rechtsetzung.

Diese Arbeitspakete werden vorrangig durch den Staat unter Mitwirkung der Unternehmen und Betreiber umgesetzt. Für den Bund koordiniert das Bundesministerium des Innern.

5. Umsetzung von Maßnahmen zur Schutzzielerreichung in erster Linie durch:
   - Verbandslösungen und interne Regelwerke,
   - Selbstverpflichtungserklärungen der Unternehmen,
   - Erarbeitung von Schutzkonzepten durch die Unternehmen.
6. Kontinuierlicher intensiver Risikokommunikationsprozess (Dialog über Analyseergebnisse, Bewertungen, Schutzziele und Maßnahmeoptionen).

Die Realisierung der Arbeitspakete 5 und 6 obliegt vorrangig den Unternehmen und Betreibern sowie Verbänden unter Beteiligung des Staates.

Zur Umsetzung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen besteht ein umfangreiches Instrumentarium in Form von

Instrumente

- Programmen und Plänen
  (z.B. der NPSI sowie die zugehörigen Umsetzungspläne als strategisches Konzept für den IT-Infrastrukturschutz),

- konkreten Handlungsempfehlungen

  (z.B. das nationale Basisschutzkonzept als grundlegende Handlungsempfehlung für den physischen Schutz Kritischer Infrastrukturen, der Leitfaden zum Risiko- und Krisenmanagement für Betreiber Kritischer Infrastrukturen oder die nationalen Spezialschutzkonzepte als detaillierte Handlungsempfehlungen für den Schutz einzelner Sektoren und Branchen Kritischer Infrastrukturen),

- sowie Standards, Normen und Regelwerke

  (z.B. die BSI-Standards zur Informationssicherheit als grundlegende Handlungsempfehlung für Betreiber Kritischer Infrastrukturen oder das Regelwerk des DVGW zum Risikomanagement im Bereich der Trinkwasserversorgung).

Die Verfahrensschritte und die Instrumente, die der Umsetzung des politisch-strategischen Rahmenkonzeptes dienen, benötigen aufgrund des gewählten und vorrangig zu verfolgenden kooperativen Ansatzes entsprechend institutionalisierte Plattformen zwischen Staat und Behörden, Unternehmen und Verbänden. Diese sicherheitspartnerschaftlichen Plattformen können organisiert sein in:

- Gesprächskreise KRITIS (Bund),
- Gesprächskreise KRITIS (Länder),
- Gesprächskreise KRITIS (Kreise und Gemeinden)

Sicherheits-partnerschaften

sowie in gemeinsamen Gesprächskreisen von Bund und Ländern bzw. von Ländern und Kommunen. Die jeweiligen Gesprächskreise sollten ihre Arbeit nach einem gemeinsam abgestimmten Verfahren organisieren, das sich inhaltlich an der Nationalen Strategie, ihrer Philosophie sowie ihrer Verfahrensschritte und Instrumentarien orientiert.

●●●

8. Internationale Zusammenarbeit

Katastrophen mit Auswirkungen auf die Funktionsfähigkeit Kritischer Infrastrukturen machen an Staatsgrenzen nicht halt, wie das Elbehochwasser 2002 nachdrücklich gezeigt hat. Zudem gewinnt der Schutz Kritischer Infrastrukturen aufgrund der international bedeutsamen Komponenten vor allem im Bereich der Informations- und Kommunikationstechnologien sowie der Energie- und Verkehrsinfrastrukturen zunehmend an grenzüberschreitender Bedeutung, die auch die Zielsetzung einer Nationalen Strategie beeinflusst und für ihre Umsetzung von Bedeutung ist.

Für Deutschland wichtige internationale Partner und Kooperationsforen sind dabei vor allem:

- die unmittelbar angrenzenden Nachbarstaaten,
- die Europäische Union,
- die G 8 – Staaten,
- die NATO.

Deutschland unterstützt im Rahmen der internationalen Zusammenarbeit alle Bemühungen und Maßnahmen, die geeignet sind, die Verletzlichkeit vor allem der grenzüberschreitend wirkenden Infrastrukturen zu erkennen und zu minimieren. Dem Ausbau bestehender und der Förderung neuer bilateraler Kooperationen zum Austausch von Informationen und „best practice“ sowie zur Abstimmung von Maßnahmen zum Schutz grenzüberschreitender Kritischer Infrastrukturen kommt eine zentrale Rolle zu.

Von besonderer Bedeutung sind Aktivitäten auf europäischer Ebene. Deutschland sieht in bilateralen und multilateralen Aktivitäten zum Schutz Kritischer Infrastrukturen wie beispielsweise dem Austausch von Informationen und Methoden sowie bewährten Verfahrensweisen den richtigen Ansatz, um die Ziele zum Schutz der Infrastrukturen im gesamten Bereich der Europäischen Union unter Wahrung des Subsidiaritätsprinzips zu verankern. Zu diesem Zweck arbeitet die Bundesregierung eng mit den Mitgliedstaaten sowie mit der Europäischen Kommission zusammen. Dabei wird sich Deutschland für die Etablierung von adäquaten Schutzstandards im europäischen Raum einsetzen und seine Konzepte und Vorstellungen zum Schutz Kritischer Infrastrukturen auf Grundlage der Nationalen Strategie nachhaltig vertreten.

●●●